Defense Travel System

DTS DBsign Client for DTS

Version 1.1

Prepared by:
Northrop Grumman Mission Systems
One Federal Systems Park Drive
Fairfax, VA 22033

Revision History

Date	Revision Number	Authorization	Revision/Change Description	Page, Section
5/08/2003	1.1	Dov Levy	Updated Section 5.2.1	Page 5
			Inserted Section 7	Page 12
			Updated Appendix A	Page A-1

Table of Contents

List of Figures

List of Tables

1 Introduction

DBsign is a commercial off-the-self (COTS) security software product used by DTS to authenticate users and sign documents. Each time an end user logs on to DTS or signs a document, DBsign is activated on the user's computer. This document provides information and recommendations for using DTS with DBsign on an end-user's computer including:

- A brief description of the military and commercial users of DBsign
- An overview of the client-side architecture of DBsign
- Concepts and issues associated with digitally signing documents
- DBsign installation and configuration

1.1 Intended Audience

This document is intended for the following categories of people:

- General DTS users – People who use DTS and, as a result, need to install and configure DBsign.
- System administrators - People who need to install and configure DBsign on behalf of DTS users, and need to understand the results of a DBsign installation on the computers that they administer.

1.2 About DBsign

Although DBsign is a commercial product, it was originally designed with DoD and the federal government in mind, and was based on Gradkell System, Inc.'s extensive experience (over 10 years) in government digital signature solutions.

DBsign is used in the Air Force's Automated Business Services System (ABSS) at over 80 Air Force bases worldwide. DBsign enabled ABSS to be the first (and currently the only) production DoD system to achieve Public Key Infrastructure (PKI) certification by DoD's Joint Interoperability Test Command (JITC). See Appendix C – DBsign JITC Certification Compliance Report and Appendix D – DBsign JITC Certification Compliance Memo for more information. The Defense Finance and Accounting Service (DFAS) is also a large DBsign customer. DFAS procured DBsign for use in the Defense Joint Accounting System (DJAS). Other agencies using digital signature solutions developed by Gradkell Systems include the Army Corps of Engineers Financial Systems (CEFMS), the Census Bureau's Travel Management Information System (TMIS), and the State Department's Electronic Certificate System. The digital signatures technology in some of these systems has received sanctioning by the General Accounting Office (GAO) as legally binding signatures. See Appendix E – GAO Sanction Letter 1 and Appendix F – GAO Sanction Letter 2 for more information.

2 Client Architecture

DBsign includes client software called the DBsign Web Signer that performs document signing using a DTS user's credentials. The following diagram illustrates the runtime environment of the DBsign Web Signer.

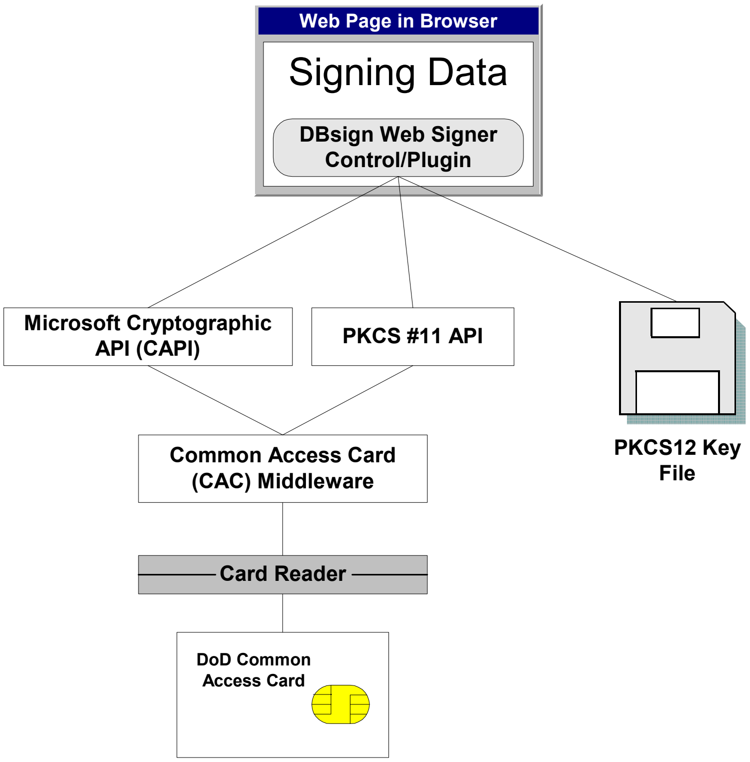

Web Page in Browser
Signing Data
DBsign Web Signer Control/Plugin
Microsoft Cryptographic API (CAPI)
PKCS #11 API
PKCS12 Key File
Common Access Card (CAC) Middleware
Card Reader
DoD Common Access Card

Figure 1 - Client Architecture

The DBsign Web Signer executes in a web browser. It can access a user's credentials via Microsoft (MS) Cryptographic Application Programming Interface (CAPI), PKCS #11 API, or PKCS #12 key files.

CAPI and PKCS #11 are Application Programming Interfaces (APIs) defined so that a user's credentials can be accessed in a standard way. Common Access Card (CAC) middleware vendors implement CAPI and PKCS #11 to provide access to credentials stored on a CAC.

PKCS #12 is a standard for storing credentials in a file. PKCS #12 files are also called key files, or soft or floppy certificates. PKCS #12 files are typically encrypted for their protection.

3 Browser Support

The DBsign Web Signer integrates with popular web browsers such as MS Internet Explorer (IE) and Netscape Navigator (NS). This browser-level integration takes place through the browser's integration APIs. For IE (and compatibles), the integration is accomplished via a "control." For

NS (and compatibles), the integration takes place through a "plugin." Regardless of which browser is being used, the DBsign Web Signer is used exactly the same way.

4 CAC PIN-Prompting

A user who signs documents using a CAC may be required to enter his or her PIN before signing. The frequency of PIN-prompting differs depending on whether DBsign is configured to use CAPI or PKCS #11. In general, PIN-prompting behavior falls into the following categories:

- A user is prompted for his/her PIN the first time the user's CAC is inserted in a reader and the user's credentials are accessed (e.g., when a user logs onto a Windows2000 workstation with a CAC, or the first time the user accesses any PK-enabled application using his/her certificate)

- A user is prompted for his/her PIN the first time a PK-enabled application is started and requires access to a user's credentials (e.g., for initial user authentication to each PK-enabled application)

- A user is prompted for his/her PIN each time a digital signing operation is performed (e.g., when a digital signature is applied within an application to which a user is already logged in)

- A user is prompted for his/her PIN after a configurable idle timeout period (i.e., if the user's credentials have not been accessed within *x* seconds or minutes, the user must re-enter his/her PIN before access to the user's credentials will be granted to the using application)

4.1.1 CAPI PIN-Prompting

When DBsign is configured to use CAPI, PIN-prompting behavior is a function of the CAC middleware, which is generally configurable. Table 1, below, summarizes the behavior for the five commonly used CAC middleware products (Spyrus, Datakey, Schlumberger, ActivCard, and SSP Litronic).

Note that many of the products support more than one PIN-prompting option. In this case, the PIN-prompting behavior will depend on the configuration of the user's middleware. Notes following the table describe the specific behavior observed with each product.

Table 1: PIN-Prompting Behavior of CAC Middleware Products

Behavior Middleware/ Certificate Format	Prompt at first access only	Prompt for each new application	Prompt for each signing operation	Prompt after inactivity period
Spyrus Rosetta Executive Suite v4		✓(1)		
Datakey CIP 4.7		✓ (2)		✓ (3)
Schlumberger CACTUS 2.0		✓ (4)		

ActivCard Gold for CAC 2.2	✓ (5)			✓ (6)
SSP Litronic NetSign CAC 3.2		✓ (7)	✓ (7)	✓ (7)

NOTES:

Spyrus

1. Spyrus will prompt a user for a PIN the first time the user's card is accessed after a new application is started. There are no other options for PIN-prompting.

Datakey

2. By default, Datakey will prompt the user for a PIN the first time the user's card is accessed after a new PK-enabled application is started.

3. Datakey can also be configured to prompt a user for a PIN if the user's card has not been accessed for at least 1 minute. Datakey's inactivity timeout period can be enabled and configured via a GUI utility provided with the middleware.

Schlumberger

4. Schlumberger will prompt the user for a PIN the first time the user's card is accessed after a new application is started. There are no other options for PIN-prompting.

ActivCard

5. By default, ActivCard will only prompt the user for a PIN the first time the user's card is accessed. No prompting occurs on subsequent card access regardless of the application in which an access occurs.

6. ActivCard can be configured to prompt a user for a PIN if the user's card has not been accessed for a configurable timeout period of at least 60 seconds. Adding the following key to the Microsoft Registry and a value in seconds configures ActivCard's inactivity timeout: HKEY_LOCAL_MACHINE\SOFTWARE\ActivCard\Gold\ACPINTO\Timeout_Idle.

SSP Litronic

7. Litronic can be configured via a GUI utility to prompt a user for a PIN the first time the user's card is accessed after a new application is started, each time the user's card is accessed and if the user's card has not been accessed for a configurable timeout period of at least 5 seconds.

The ability of DTS to prompt for a PIN when DBsign is configured to use CAPI depends on the type of middleware used and its configuration. Only the SSP Litronic middleware provides the option to prompt the user for a PIN each time a signing operation is performed.

4.1.2 PKCS #11 PIN-Prompting

When DBsign is configured to use PKCS #11, a user is prompted for his/her PIN each time a digital signing operation is performed. PIN-prompting behavior is a function of DBsign, which implements this behavior.

5 DBsign Installation

Before DTS can be used, the DBsign Web Signer must be installed. DBsign supports two mechanisms for installing the DBsign Web Signer:

1. MS Internet Component Download (MSICD)

2. DBsign installation program

Because installation of the DBsign Web Signer requires administrator privileges, DTS only supports installation via the DBsign installation program.

5.1 MSICD

MSICD is a MS service supported by IE for downloading and installing software from Web sites. Because installation requires that a user downloading and installing software have administrator privileges on his or her computer, DTS does not use this installation option. Consequently, there are no issues involved with DTS and mobile code.

5.2 Installation Program

DBsign Web Signer includes an installation program. The program is a single file executable installer developed using InstallShield Professional 7 and packaged with InstallShield's PackageForTheWeb. This combination of products yields an install program that can be executed standalone, via a web link, or delivered silently and automatically through automated software distribution products such as SMS. This program may only be run by someone logged on as a user with administrator privileges.

5.2.1 Silent Install

The DBsign Web Signer's installation program can be used in either interactive or silent mode. Silent installs are initiated by specifying a response script (see APPENDIX A for a sample) to the DBsign installation program.

A response script is created in the interactive mode. It contains the information for which a user installing DBsign would normally be prompted. The instructions for creating and using a response script with the DBsign installation program are as follows:

To create a response script, do the following:

1. Determine how DBsign should be configured. Your options are:

- Default Configuration – Use this configuration if you want DBsign to get a user's credentials from the MS CAPI store (e.g., CACs or imported credentials), or secondarily to prompt for a soft certificate.

- Advanced Configuration – Advanced configuration includes two options as follows:

    - PKCS12 – Use this configuration if you want DBsign to exclusively prompt for a soft certificate. With this option, DBsign will not use CAPI.

    - PKCS11 – Use this configuration if you want DBsign to use the P11 drivers provided by a CAC middleware vendor to get a user's credentials. This option is rarely used since the default option supports CACs.

See Section 6 for more information on DBsign configuration options.

2. Determine the directory where DBsign should be installed.

3. Run the DBsign installation program (i.e., DBsignWebSigner.exe) so that it not only installs DBsign but also creates a response script that captures the decisions made during installation (see steps 1 and 2).

   To create a response script use the following switches when invoking the DBsign installation program:

   - –r – Tells the DBsign installation program to create a response script

   - -f1<response script file name> – Tells the DBsign installation program where to write the response script file. This switch must include the fully qualified name of the response file. (Note: Do not include a space between the switch and the file name.)

   The following is an example of how to run DBsignWebSigner.exe so that it creates a response script:

   - DBsignWebSigner.exe -r -f1"d:\temp\DBsignInstall\DBsignInstall.iss"

After running the install program, the DBsign should be installed on the computer and should have a response script at the location specified by the "-f1" switch.

To install DBsign in silent mode, do the following:

1. Run the DBsign installation program (i.e., DBsignWebSigner.exe) so that it runs silently (i.e., without requiring user input) and uses a response script. To install in silent mode, use the following switches:

   - -s – Tells the DBsign installation program to run in silent mode

   - -f1<response script name> – Tells the DBsign installation program the location of the response script. This switch must include the fully qualified name of the response file. (Note: Do not include a space between the switch and the file name.)

The following is an example of how to run DBsignWebSigner.exe so that it runs in silent mode from a response script:

- DBsignWebSigner.exe -s -f1"d:\temp\DBsignInstall\DBsignInstall.iss"

After running the DBsign installation program in silent mode, DBsign should be installed on the computer.

5.2.2 Installed Files

The DBsign installation program installs the following files on a user's computer:

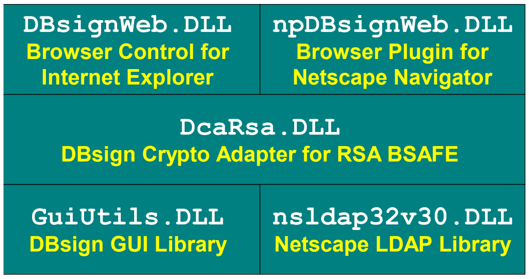

DBsignWeb.DLL
Browser Control for Internet Explorer
npDBsignWeb.DLL
Browser Plugin for Netscape Navigator
DcaRsa.DLL
DBsign Crypto Adapter for RSA BSAFE
GuiUtils.DLL
DBsign GUI Library
nsldap32v30.DLL
Netscape LDAP Library

Figure 2 - DBsign Web Signer Components

- DBsignWeb.DLL or npDBsignWeb.DLL: These are the browser integration components. The IE control is implemented in DBsignWeb.DLL. The NS plugin is implemented in npDBsignWeb.DLL (plugin library file names must always begin with the letters "np").

- DcaRsa.DLL: The DBsign Crypto Adapter for RSA BSAFE. This library is one of the DBsign cryptographic library implementations. DcaRsa.DLL uses the BSAFE cryptographic toolkit from RSA Security Inc. (FIPS 140-1 Validation Certificate #163).

- GuiUtils.DLL: This library performs all functions that involve GUI-related operations. Since DBsign operates in multiple hardware and operating system platforms, all GUI related operations are consolidated in this library.

- Nsldap32v30.dll: This is the library used by DBsign to interact with LDAP directories.

5.2.3 MS Registry

A number of entries are added to the MS Registry during the installation of DBsign Web Signer.

To support installation and de-installation, InstallShield Professional 7, which is the basis of the DBsign installation program, adds the following registry entry:

- HKEY_LOCAL_MACHINE\SOFTWARE\Gradkell Systems, Inc.\DBsign Web Signer\<version number>

  "version number" corresponds to the version installed on the user's computer

To support DBsign user-level and computer-level configuration, the DBsign installation program adds the following registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE \Gradkell Systems, Inc.\DBsign Data Security Suite\Client Settings\Crypto Settings - *For computer-level configuration*

- HKEY_CURRENT_USER\Software\Gradkell Systems, Inc.\DBsign Data Security Suite\Client Settings\Crypto Settings - *For user-level configuration*

The keys above enable a configuration to be applied to a computer or a specific user. The configuration for users who do not have a user-level configuration (e.g., users that had DBsign installed by an administrator) is determined by the computer-level configuration. When defined, user-level configuration overrides computer-level configuration for a specific user.

Under the computer-level and user-level keys described above, the DBsign installation program adds the following entries:

- DBS_USE_CAPI: Toggles the use of CAPI. If this value is set to “1”, DBsign will use CAPI to access a user’s credentials when logging on and document signing. This setting defaults to “1”.

- DBS_USE_KEY_FILE: Toggles the use of key files (i.e., PKCS #12 files). If this value is set to “1”, DBsign will prompt the user for a key file and a password when logging on and document signing. This setting defaults to “0”.

- DBS_USE_PKCS11: Toggles the use of CAC middleware vendor provided PKCS #11 drivers. If this value is set to “1”, DBsign will use PKCS #11 to access a user’s credentials when logging on and document signing. This setting defaults to “0”.

- DBS_KEY_FILE_NAME: Specifies the full path and file name of the key file to use. This setting is used in combination with the DBS_REMEMBER_KEY_FILE_NAME setting. There is no default for this setting.

- DBS_REMEMBER_KEY_FILE_NAME: Specifies whether or not to remember the key file name between prompts. If set to “1”, the value of DBS_KEY_FILE_NAME will be the filled in the key file prompt dialog. If set to “0”, the user must select a key file before each DBsign login. This setting defaults to “0”.

- DBS_PKCS11_LIBRARY: Specifies the full path and file name of the PKCS #11 driver DLL that is used by DBsign and is provided by a CAC middleware vendor. There is no default for this setting.

DBsign registry entries are removed when DBsign is uninstalled.

6 DBsign Configuration

DBsign can be configured to use CAPI, PKCS #11 or PKCS #12 when accessing a user’s credentials. Configuration occurs at installation time via the installation program or sometime afterward via the DBsign Client Configuration Utility.

6.1 Installation-time Configuration

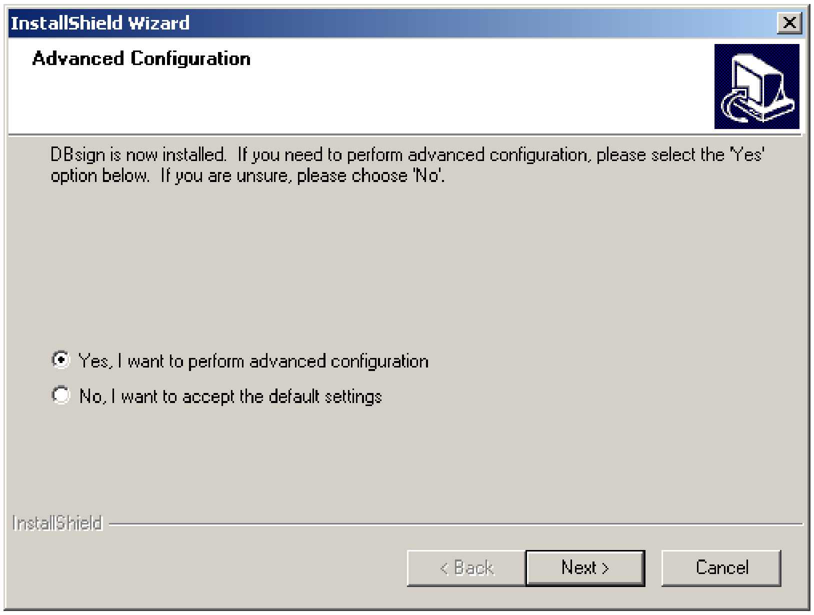
The DBsign default configuration results when all of the default settings are selected during installation. The default configuration enables the DBsign Web Signer to access a user's credentials via CAPI. Also, DTS uses a DBsign feature that enables it to prompt for the location of a PKCS #12 file in the event that no signing certificates are available via CAPI. As a result, the default configuration is satisfactory for users that have their credentials stored on a CAC or have their credentials stored in a file on the hard disk or on a floppy. The default configuration is the least complicated to perform and should be sufficient for most users.

6.1.1 Advanced Configuration

Users have the option of performing advanced configuration if the default configuration is not satisfactory. Examples where users might perform advanced configuration include:

- Users who have their credentials stored on a CAC and are required by their organization to provide a PIN each time they sign a document and their CAC middleware does not support this option.
- Users who want their credentials to be accessed from only one source such as only PKCS #12.

Advanced configuration occurs during installation via the Advanced Configuration dialog window illustrated in Figure 3. The Advanced Configuration dialog window enables a user to start the advanced configuration process by selecting "Yes, I want to perform advanced configuration" and then selecting "Next". Note that selecting "No, I want to accept the default settings" results in the DBsign default configuration.



InstallShield Wizard

Advanced Configuration

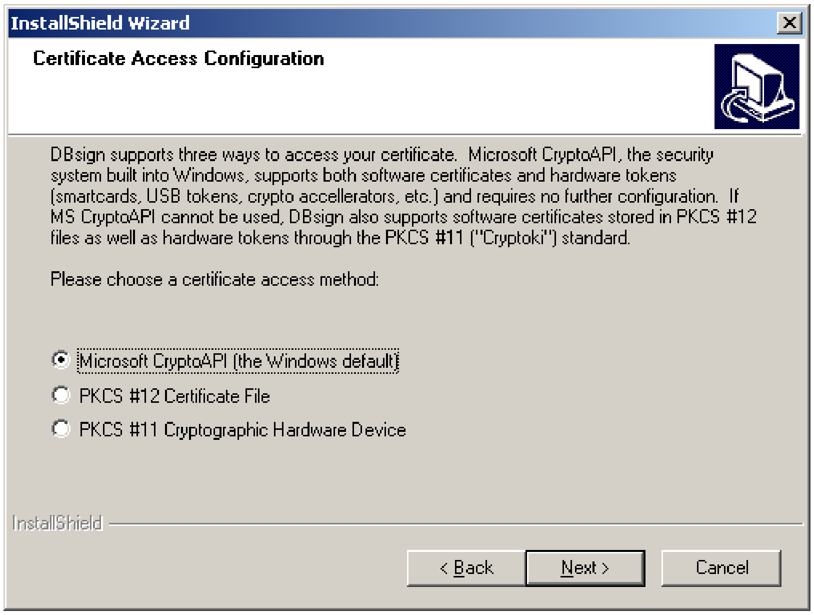
DBsign is now installed. If you need to perform advanced configuration, please select the 'Yes' option below. If you are unsure, please choose 'No'.

● Yes, I want to perform advanced configuration

○ No, I want to accept the default settings

Figure 3 - DBsign Advanced Configuration

If a user selects “Yes, I want to perform advanced configuration” and then selects the “Next” button, the user is presented with the Certificate Access Configuration dialog illustrated in Figure 4. This dialog allows a user to configure DBsign to use CAPI, PKCS #12 or PKCS #11.



InstallShield Wizard

Certificate Access Configuration

DBsign supports three ways to access your certificate. Microsoft CryptoAPI, the security system built into Windows, supports both software certificates and hardware tokens (smartcards, USB tokens, crypto accellerators, etc.) and requires no further configuration. If MS CryptoAPI cannot be used, DBsign also supports software certificates stored in PKCS #12 files as well as hardware tokens through the PKCS #11 ("Cryptoki") standard.

Please choose a certificate access method:

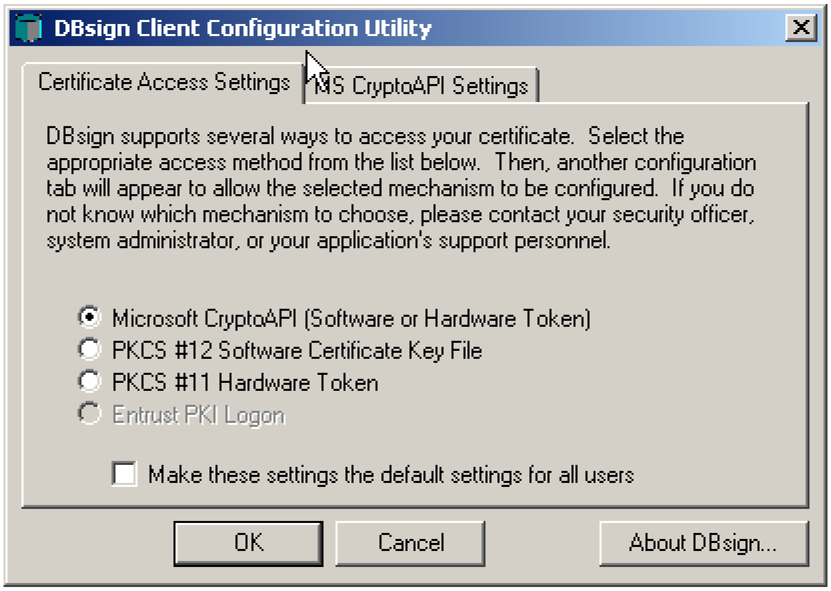
● Microsoft CryptoAPI (the Windows default)
○ PKCS #12 Certificate File
○ PKCS #11 Cryptographic Hardware Device

Figure 4 - Certificate Access Configuration

If PKCS #11 is selected, the user is presented with a dialog window in which to enter the fully qualified name and location of the PKCS #11 driver provided by the CAC middleware vendor. If PKCS #12 is selected, the user is presented with a dialog window in which to enter the fully qualified name and location of his or her PKCS #12 file.

6.2 Client Configuration Utility

If a user wants to reconfigure DBsign after installation, then the DBsign Client Configuration Utility, illustrated in Figure 5 and included at installation, must be run.


DBsign Client Configuration Utility
Certificate Access Settings
MS CryptoAPI Settings
OK
Cancel
About DBsign...

DBsign supports several ways to access your certificate. Select the appropriate access method from the list below. Then, another configuration tab will appear to allow the selected mechanism to be configured. If you do not know which mechanism to choose, please contact your security officer, system administrator, or your application's support personnel.

● Microsoft CryptoAPI (Software or Hardware Token)
○ PKCS #12 Software Certificate Key File
○ PKCS #11 Hardware Token
○ Entrust PKI Logon

□ Make these settings the default settings for all users

Figure 5 - Client Configuration Utility

DBsign Client Configuration Utility enables a user to specify that the DBsign Web Signer should use one of the following when signing documents:

- Microsoft CryptoAPI – For accessing credentials stored on a hardware token such as a CAC or in the IE browser certificate store. When this option is selected, no additional settings are available. The MS CryptoAPI Settings tab in the figure is strictly informational.

- PKCS #12 – For accessing credentials stored in a file on a floppy or the hard disk. When this option is selected, the user is presented with a tab in which to enter the fully qualified name and location of the key file.

- PKCS #11 – For accessing credentials stored in a hardware token such as a CAC specifically using PKCS #11 drivers provided by a CAC middleware vendor. When this option is selected, the user is presented with a tab in which to enter the fully qualified name and location of the PKCS #11 driver.

The "Make these settings the default settings for all users" check box is used to indicate if the configuration should be applied to just the user, or both the user and the computer. When checked, the configuration is applied to both the user and computer.

7 Troubleshooting

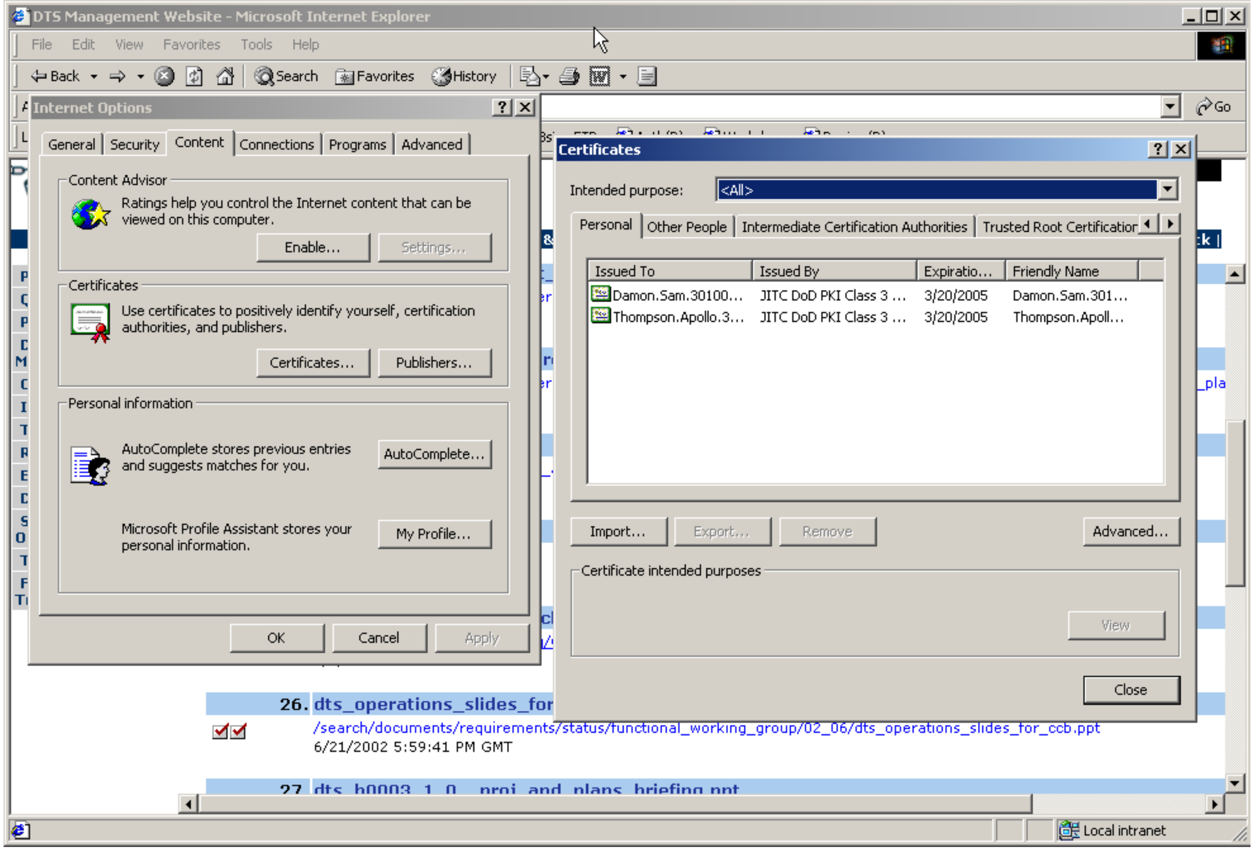
This section presents troubleshooting information. Use this information to diagnose common DTS login problems.

7.1 Problem: DBsign is not using your CAC

In the default configuration, DBsign uses CAPI to access a user's credentials stored, for example, on a CAC. If you're using a CAC and you're getting prompted for a soft certificate, your certificates are probably not registered into CAPI. This problem may exist even if your certificates appear to be in CAPI.

7.1.1 Ensure CAC certificates are registered

Do the following to verify that the certificates on your CAC have been registered to CAPI. In MS IE, select Tools->Internet Options->Content->Certificates… as illustrated in Figure 6. If no certificates appear in the Personal tab, then the certificates on your CAC have not been registered into CAPI. If your certificates appear in the certificate list but are not accessed by DBsign, you may need to delete them from the list and re-register them as described in 7.1.2.



DTS Management Website - Microsoft Internet Explorer

Internet Options

Content Advisor

Ratings help you control the Internet content that can be viewed on this computer.

Certificates

Use certificates to positively identify yourself, certification authorities, and publishers.

Personal information

AutoComplete stores previous entries and suggests matches for you.

Microsoft Profile Assistant stores your personal information.

Certificates

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Damon.Sam.30100...	JITC DoD PKI Class 3 ...	3/20/2005	Damon.Sam.301...
Thompson.Apollo.3...	JITC DoD PKI Class 3 ...	3/20/2005	Thompson.Apoll...

Certificate intended purposes

26. dts_operations_slides_for
/search/documents/requirements/status/functional_working_group/02_06/dts_operations_slides_for_ccb.ppt
6/21/2002 5:59:41 PM GMT

27. dts_h0003_1_0__proj_and_plans_briefing.ppt

Figure 6 - MS Certificate Browser

7.1.2 Registering CAC certificates

The process of registering certificates stored on a CAC to CAPI varies among CAC middleware vendors. A middleware vendor will usually provide a utility to access your CAC. The utility will usually include an option to register, import or migrate your certificates from your CAC to CAPI. The registration process will only register public information such as certificate information and not private information such as private keys.

For example, to register your certificates using ActivCard Gold for CAC 2.2, bring up the ActivCard Gold Utilities application illustrated in Figure 7.

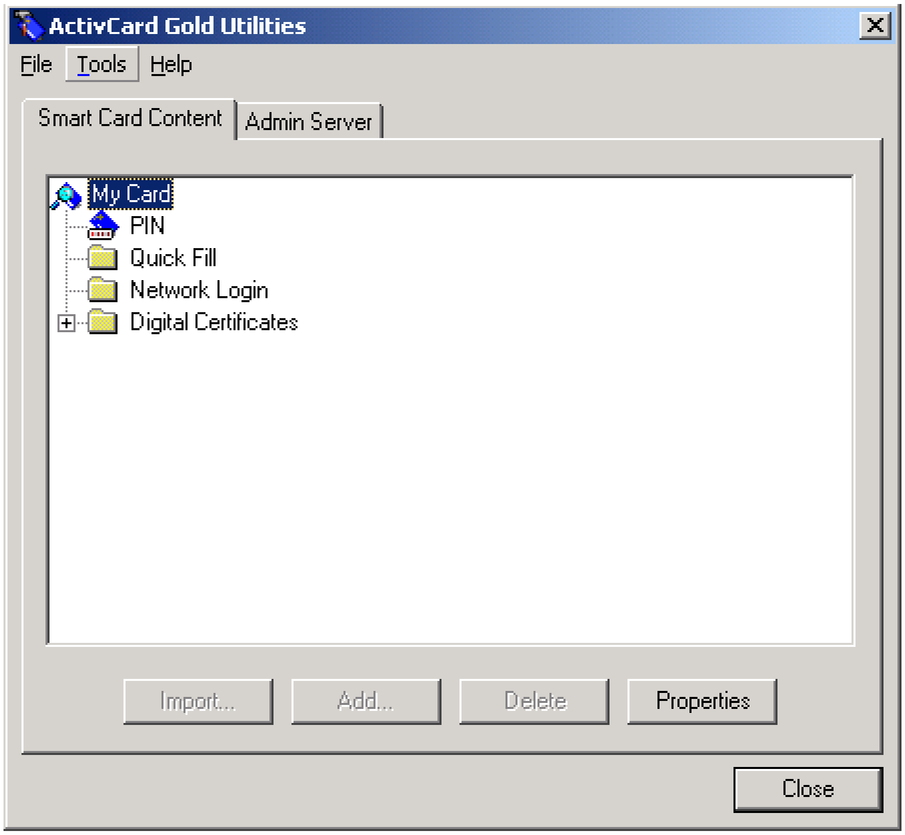
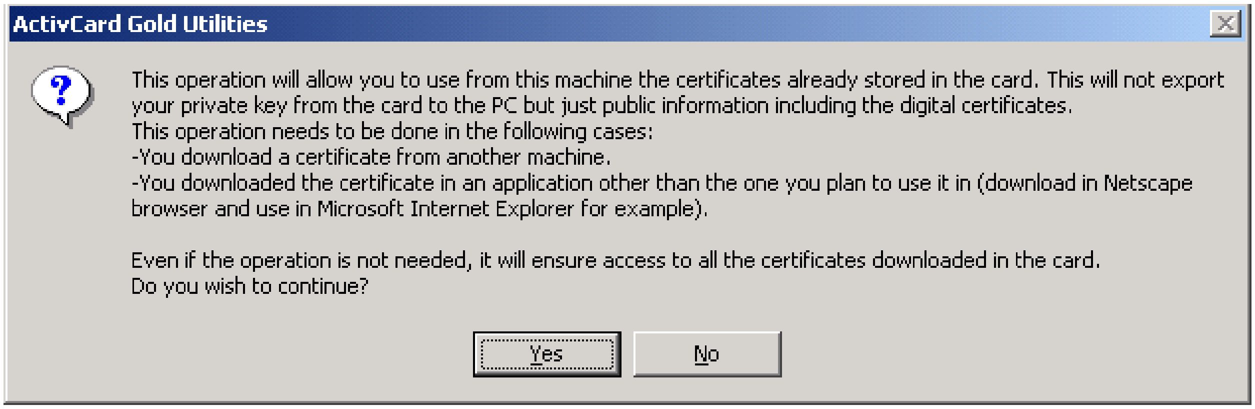


Figure 7 - ActivCard Gold Utilities

In the ActivCard Gold Utilities window, select the Tools->Register Certificates… option. The dialog window illustrated in Figure 8 will appear. Select **Yes** to have your certificates registered to CAPI.

See your CAC middleware vendor end-user documentation from more information.



This operation will allow you to use from this machine the certificates already stored in the card. This will not export your private key from the card to the PC but just public information including the digital certificates.
This operation needs to be done in the following cases:
-You download a certificate from another machine.
-You downloaded the certificate in an application other than the one you plan to use it in (download in Netscape browser and use in Microsoft Internet Explorer for example).

Even if the operation is not needed, it will ensure access to all the certificates downloaded in the card.
Do you wish to continue?

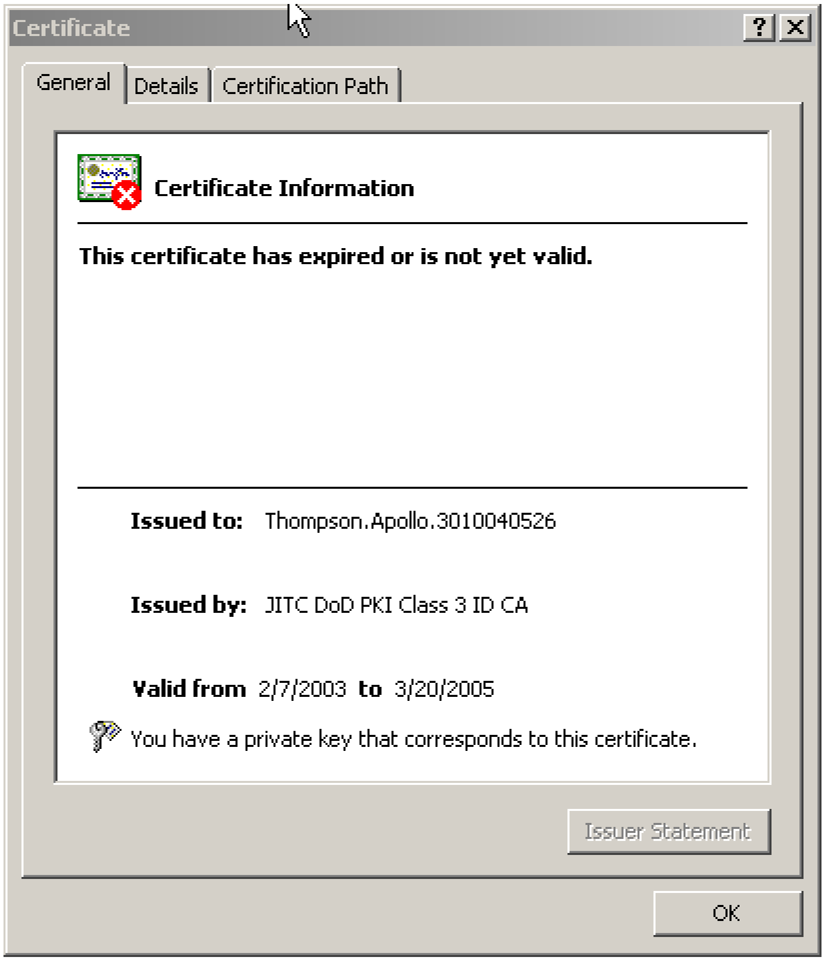
Figure 8 - CAC Registration Verification Prompt

7.2 Problem: DBsign repeatedly prompts for a soft certificate

If DBsign repeatedly prompts for a soft certificate when you're trying to access DTS, then DBsign is refusing to accept your certificate because of a problem. If this occurs, you can import the certificate into CAPI and check it for errors.

7.2.1 Verify that the certificate is valid

You can verify that a certificate is valid by importing it into CAPI. To import a certificate, use the Import button in the Certificate browser window illustrated in Figure 6. Selecting the Import button activates the Certificate Import Wizard. Complete the series of dialogs to import your certificate. After your certificate is imported, you should be able to see it in the certificate list. If you double-click the certificate, a Certificate details window will appear as illustrated in Figure 9. For example, the information in Figure 9 indicates that the certificate has expired. In this case, the certificate has expired because the date on the computer has been set back.



Certificate Information

This certificate has expired or is not yet valid.

Issued to: Thompson.Apollo.3010040526

Issued by: JITC DoD PKI Class 3 ID CA

Valid from 2/7/2003 to 3/20/2005

You have a private key that corresponds to this certificate.

Figure 9 - Certificate Details

Note that after a certificate has been imported and verified, it should be removed from the certificate list to prevent misuse.

7.2.2 Ensure that DTS is configured to support the issuer of your credentials

In some cases, DBsign may reject a certificate because the certificate's issuer is not known to DTS. If your certificate is valid and the repeated prompting continues, then you'll need to contact the DTS helpdesk to ensure that DTS supports the issuer of your certificate. You can use the Certificate Details dialog illustrated in Figure 9 to determine your issuer.

7.3 Problem: DBsign does not prompt for a soft certificate password

If you're able to access DTS without getting prompted for a password, then your certificate has probably been imported into CAPI in low security mode. Importing your certificate into CAPI in low security mode will enable its access without requiring a password. You should remove the certificate from the CAPI store as described below. If you need to retain the certificate in CAPI for some reason, you can export it and then re-import it in high security mode to force a password prompt when the certificate is accessed.

7.3.1 Ensure that your soft certificate is not in CAPI

To ensure that your soft certificate has not been inadvertently imported into CAPI, use the Certificate browser as illustrated in Figure 6. Certificates imported into CAPI are listed in the Personal tab. To remove a certificate, select it in the Personal tab and then select the Remove button. Be careful not to remove any certificates that are legitimately in CAPI, such as those used for email or those registered by CAC middleware.

APPENDIX A

Sample Response Script

Appendix A – Sample Response Script

The following illustrates a sample response script. A response script is used to run the DBsign installation program in silent-mode. The response script below appears strictly for illustrative purposes. Because the DBsign installation program is subject to change independent of this document, the sample below should not be used directly. A new response script should be created using the steps in section 5.2.1.

```
[InstallShield Silent]
Version=v7.00
File=Response File
[File Transfer]
OverwrittenReadOnly=NoToAll
[{44D21B77-D4FC-49E8-A726-CD00D5016703}-DlgOrder]
Dlg0={44D21B77-D4FC-49E8-A726-CD00D5016703}-SdWelcome-0
Count=9
Dlg1={44D21B77-D4FC-49E8-A726-CD00D5016703}-SdLicense2-0
Dlg2={44D21B77-D4FC-49E8-A726-CD00D5016703}-SdAskDestPath2-0
Dlg3={44D21B77-D4FC-49E8-A726-CD00D5016703}-SdStartCopy2-0
Dlg4={44D21B77-D4FC-49E8-A726-CD00D5016703}-SdAskOptions-0
Dlg5={44D21B77-D4FC-49E8-A726-CD00D5016703}-SdAskOptions-1
Dlg6={44D21B77-D4FC-49E8-A726-CD00D5016703}-SdShowDlgEdit1-0
Dlg7={44D21B77-D4FC-49E8-A726-CD00D5016703}-SdShowInfoList-0
Dlg8={44D21B77-D4FC-49E8-A726-CD00D5016703}-SdFinishReboot-0
[{44D21B77-D4FC-49E8-A726-CD00D5016703}-SdWelcome-0]
Result=1
[{44D21B77-D4FC-49E8-A726-CD00D5016703}-SdLicense2-0]
Result=1
[{44D21B77-D4FC-49E8-A726-CD00D5016703}-SdAskDestPath2-0]
szDir=C:\Program Files\Gradkell Systems, Inc\DBsign Web Signer
Result=1
[{44D21B77-D4FC-49E8-A726-CD00D5016703}-SdStartCopy2-0]
Result=1
[Application]
Name=DBsign Web Signer
Version=2.3
Company=Gradkell Systems, Inc.
Lang=0009
[{44D21B77-D4FC-49E8-A726-CD00D5016703}-SdAskOptions-0]
Component-type=string
Component-count=1
Component-0=Yes, I want to perform advanced configuration
Result=1
[{44D21B77-D4FC-49E8-A726-CD00D5016703}-SdAskOptions-1]
Component-type=string
Component-count=1
Component-0=PKCS #12 Certificate File
Result=1
[{44D21B77-D4FC-49E8-A726-CD00D5016703}-SdShowDlgEdit1-0]
szEdit1=' '
Result=1
[{44D21B77-D4FC-49E8-A726-CD00D5016703}-SdShowInfoList-0]
Result=1
[{44D21B77-D4FC-49E8-A726-CD00D5016703}-SdFinishReboot-0]
Result=1
BootOption=0
```

APPENDIX B

CAC Compatibility Tests Results

Appendix B – CAC Compatibility Tests Results

This section presents the results of DBsign and CAC compatibility testing. Each table contains the test results for a particular platform where each cell indicates whether the test for a particular CAC middleware and Web browser combination succeeded or not. Additional analysis is being performed in those cases where a test did not succeed. Please note the following:

- Except where noted, DBsign was configured to access a CAC using CAPI and not PKCS #11.
- In some cases a manual registration of a CAC's certificates to CAPI were required.
- Many of the tests were performed using an Oberthur v4 CAC that is not supported by ActivCard 2.1.

Windows 2000

	ActivCard 2.1	ActivCard 2.2	Datakey	Litronic	Schlumberger	Spyrus
Internet Explorer (6.0)	YES	YES	YES	YES (1)	YES	YES
Netscape (6.2.3)	YES	YES	YES	YES (1)	YES	YES

1. Certificates were imported using the CAC Browser and not the Register IE Card feature.

Windows NT 4

	ActivCard 2.1	ActivCard 2.2	Datakey	Litronic	Schlumberger	Spyrus
Internet Explorer (5.5)	NO (1)	YES	YES	YES	YES	YES
Netscape (6.2.3)	NO (1)	YES	YES	YES	YES	YES

1. Tested with an Oberthur V4 CAC, which is not supported by ActivCard 2.1.

Windows XP Pro

	ActivCard 2.1	ActivCard 2.2	Datakey	Litronic	Schlumberger	Spyrus
Internet Explorer (5.5)	NO(1)	YES	YES	YES	YES	YES

Netscape (6.2.3)	NO(1)	YES	YES	YES	YES	YES

1. Tested with an Oberthur V4 CAC, which is not supported by ActivCard 2.1.

Windows 98

	ActivCard 2.1	ActivCard 2.2	Datakey	Litronic	Schlumberger	Spyrus
Internet Explorer (5.5)	NO (1)	YES	YES	YES	YES	YES
Netscape (6.2.3)	NO (1)	YES	YES	YES	YES	YES
Netscape (4.79)	NO (1)	YES	YES	YES	YES	YES

1. ActivCard 2.1 failed to install correctly.

APPENDIX C

DBsign JITC Certification Compliance Report

Appendix C – DBsign JITC Certification Compliance Report

"DBsign Certification
Compliance Testing S

APPENDIX D

DBsign JITC Certification Compliance Memo

Appendix D – DBsign JITC Certification Compliance Memo

dbsign_jul_memo.pdf

APPENDIX E

GAO Sanction Letter 1

Appendix E – GAO Sanction Letter 1

Gao_Corps.pdf

APPENDIX F

GAO Sanction Letter 2

Appendix F – GAO Sanction Letter 2

Gao_State.pdf